On page 9, lines 31-32, replace "(3), above" with --(4), reprinted below--.

On page 9, line 32, replace "M = C^d mod n" with --M $\equiv$ C^d (mod n)--.

On page 10, line 9, between "to" and "(3)", insert --relationship--.

On page 10, line 16, replace "M = C^d (mod n)" with --M $\equiv$ C^d (mod n)--.

On page 10, lines 19-27, replace

$$"M_1 = C_1^{d_1} \bmod p_1$$
$$M_2 = C_2^{d_2} \bmod p_2$$
$$M_3 = C_3^{d_3} \bmod p_3$$

where

$$C_1 = C \bmod p_1;$$
$$C_2 = C \bmod p_2;$$
$$C_3 = C \bmod p_3;$$
$$d_1 = d \bmod (p_1 - 1);$$
$$d_2 = d \bmod (p_2 - 1); \text{ and}$$
$$d_3 = d \bmod (p_3 - 1)."$$

with

$$M_1 \equiv C_1^{d_1} (\bmod \ p_1),$$
$$M_2 \equiv C_2^{d_2} (\bmod \ p_2),$$
$$M_3 \equiv C_3^{d_3} (\bmod \ p_3), \cdot$$

where

$$C_1 \equiv C (\bmod \ p_1),$$
$$C_2 \equiv C (\bmod \ p_2),$$
$$C_3 \equiv C (\bmod \ p_3),$$

$$d_1 \equiv d (\bmod \ (p_1 - 1)),$$
$$d_2 \equiv d (\bmod \ (p_2 - 1)), \text{ and}$$
$$d_3 \equiv d (\bmod \ (p_3 - 1)).$$

On page 11, lines 3-6, replace

$$"Y_i = Y_{i-1} + [(M_i - Y_{i-1}) (W_i^{-1} \bmod p_i) \bmod p_i] \cdot W_i \bmod n$$

where
$$i \geq 2 \text{ and}$$

$$M = Y_k, Y_1 = C_1, \text{ and } W_i = \prod_{j<i} p_j."$$

with "$Y_i \equiv Y_{i-1} + [(M_i - Y_{i-1}) (w_i^{-1} \bmod p_i) \bmod p_i] \cdot w_i \bmod n$
where

-2-

$2 \le i \le k,$ and

$$M = Y_k, Y_1 = M_1, \text{ and } w_i = \prod_{j<i} p_j."$$

On page 11, lines 12-21, replace

$$"C_1 = M_1^{e_1} \bmod p_1$$
$$C_2 = M_2^{e_2} \bmod p_2$$
$$C_3 = M_3^{e_3} \bmod p_3$$

where

$$M_1 = M \ (mod \ p_1),$$
$$M_2 = M \ (mod \ p_2),$$
$$M_3 = M \ (mod \ p_3),$$
$$e_1 = e \ mod \ (p_1 - 1),$$
$$e_2 = e \ mod \ (p_2 - 1), \text{ and}$$
$$e_3 = e \ mod \ (p_3 - 1)"$$

with

$$C_1 \equiv M_1^{e_1} \ (mod \ p_1)$$
$$C_2 \equiv M_2^{e_2} \ (mod \ p_2)$$
$$C_3 \equiv M_3^{e_3} \ (mod \ p_3)$$

where

$$M_1 \equiv M \ (mod \ p_1),$$
$$M_2 \equiv M \ (mod \ p_2),$$
$$M_3 \equiv M \ (mod \ p_3),$$
$$e_1 \equiv e \ (mod \ (p_1 - 1)),$$
$$e_2 \equiv e \ (mod \ (p_2 - 1)), \text{ and}$$
$$e_3 \equiv e \ (mod \ (p_3 - 1)).$$

On page 11, line 21, replace "decrypted message M" with --encrypted message C--.

On page 12, lines 3-5, replace

$$"M = \sum_{i=1}^{k} M_i (W_i^{-1} \bmod p_i) W_i \bmod n$$

where

$$W_i = \prod_{j \ne 1} p_j, and"$$

with

$$-- M \equiv \sum_{i=1}^{k} M_i (w_i^{-1} \bmod p_i) w_i \bmod n$$